

Please amend the present application as follows:

Claims

The following is a copy of Applicant's claims that identifies language being added with underlining ("___") and language being deleted with strikethrough ("—"), as is applicable:

1. (Previously presented) A method for securely transmitting data between a computer and a printer, comprising:

adding a header to a file that contains data to be printed;

providing an identifier in said header that identifies an encryption algorithm;

encrypting the file with the encryption algorithm without encrypting the header; and

transmitting said encrypted file and said unencrypted header to the printer.

2. (Previously presented) The method of claim 1, further comprising receiving said encrypted file and said unencrypted header with the printer, identifying the encryption algorithm with the printer, selecting an appropriate decryption algorithm with the printer; and decrypting said encrypted file with the printer using the decryption algorithm.

3. (Previously presented) The method of claim 1, further comprising, prior to said encrypting, converting said file into at least one of a postscript format, a PCL format, a PDF format, and an XML format.

4. (Previously presented) The method of claim 1, further comprising: receiving said encrypted file and said unencrypted header with the printer, recognizing said identifier from said

unencrypted header with the printer, validating said identifier on the printer, and selecting with the printer an appropriate decryption algorithm that is associated with the encryption algorithm.

5. (Previously presented) The method of claim 1, wherein said providing includes providing said unencrypted header with a flag recognizable solely by the printer that identifies the encryption algorithm.

6. (Canceled)

7. (Previously presented) The method of claim 5, further comprising recognizing said flag with the printer and selecting an appropriate decryption algorithm based on said recognizing.

8. (Previously presented) The method of claim 7, further comprising validating said flag on the printer by receiving a decryption key with the printer that corresponds to said flag.

9. (Canceled)

10. (Previously presented) The method of claim 7, wherein selecting an appropriate decryption algorithm comprises selecting an appropriate decryption algorithm from a plurality of decryption algorithms available to the printer.

11-16. (Canceled)

17. (Previously presented) A system for securely transmitting a file in a computer network, comprising:

a first device including at least one processor for providing a file containing data to be printed with a header that includes an identifier that identifies an encryption algorithm, and for encrypting the file with the encryption algorithm without encrypting the file header; and

a second device including at least one processor for decrypting and outputting the file.

18. (Canceled)

19. (Previously presented) The system of claim 17, wherein said at least one processor of said first device is configured to provide the file header with a flag that identifies the encryption algorithm.

20. (Previously presented) The system of claim 19, wherein said second device further includes an input element for receiving a decryption key for recognition by said at least one processor of said second device and for corresponding to at least one decryption algorithm available to said at least one processor of said second device and said flag accompanying the file.

21. (Previously presented) The system of claim 17, wherein said first device comprises a computer and said second device comprises a printer, said first device having apparatus for converting the file into a printer description language format.

22. (Previously presented) The system of claim 17, wherein said second device includes at least one decryption algorithm that corresponds to the encryption algorithm.

23. (Previously presented) A printer, comprising:
at least one processor configured to receive an encrypted file for printing and configured to read an identifier provided in an unencrypted header associated with said encrypted file, the identifier providing an indication of an encryption algorithm that was used to encrypt said file, said at least one processor being configured to execute a decryption algorithm associated with the encryption algorithm to decrypt said encrypted file; and
at least one printing element for printing said file.

24. (Original) The printer of claim 23, further comprising a memory connected to said at least one processor for storage of said decryption algorithm.

25-26. (Canceled)

27. (Previously presented) The printer of claim 23, wherein said at least one processor selects the decryption algorithm for decrypting said encrypted file from a plurality of available decryption algorithms based upon said identifier.

28. (Previously presented) The printer of claim 23, further comprising an input element configured for receiving a decryption key, said decryption key corresponding to said identifier.

29. (Previously presented) The printer of claim 28, wherein said decryption key facilitates activation of the decryption algorithm.